Groupe de travail Réseau
**Request for Comments: 5520**
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

R. Bradford, éd., Cisco Systems, Inc.
JP. Vasseur, Cisco Systems, Inc.
A. Farrel, Old Dog Consulting
avril 2009

# Préservation de la confidentialité de la topologie dans le calcul de chemin inter-domaines en utilisant un mécanisme fondé sur une clé de chemin



**Résumé**
Les chemins de commutation d'étiquettes (LSP, *Label Switched Path*) de commutation d'étiquettes multi protocoles (MPLS, *Multiprotocol Label Switching*) et de MPLS généralisé (GMPLS, *Generalized MPLS*) à ingénierie du trafic (TE, *Traffic Engineering*) peuvent être calculés par des éléments de calcul de chemin (PCE, *Path Computation Element*). Lorsque le LSP TE traverse plusieurs domaines, comme des systèmes autonomes (AS, *Autonomous System*) le chemin peut être calculé par plusieurs PCE qui coopèrent, chacun étant responsable du calcul d'un segment du chemin. Cependant, dans certains cas (par exemple, quand des AS sont administrés par des fournisseurs de service différents) cela violerait les règles de confidentialité qu'un PCE fournisse un segment de chemin à un PCE dans un autre domaine, divulguant ainsi des informations de topologie interne de l'AS. Ce problème peut être contourné en retournant un bond lâche et en invoquant un nouveau calcul de chemin à partir du routeur de commutation d'étiquettes (LSR, *Label Switching Router*) de frontière du domaine durant l'établissement du LSP TE lorsque le message de signalisation entre dans le second domaine, mais cette technique pose plusieurs problèmes incluant le problème du maintien de la diversité de chemins.

Le présent document définit un mécanisme pour cacher le contenu d'un segment d'un chemin, appelé le segment de chemin confidentiel (CPS, *Confidential Path Segment*). Le CPS peut être remplacé par une clé de chemin *(path-key)* qui peut être portée dans le protocole de communication de PCE (PCEP, *PCE Communication Protocol*) et signalé dans un objet de chemin explicite du protocole de réservation de ressource d'ingénierie du trafic (RSVP-TE, *Resource Reservation Protocol TE*).

## Table des matières

## 1. Introduction

Les techniques de calcul de chemin en utilisant l'élément de calcul de chemin (PCE, *Path Computation Element*) sont décrites dans la [RFC4655] et permettent un calcul de chemin pour les chemins de commutation d'étiquettes (LSP, *Label Switched Path*) dans l'ingénierie du trafic (TE, *Traffic Engineering*) inter domaines de commutation d'étiquettes multi protocoles (MPLS, *Multiprotocol Label Switching*) et de MPLS généralisé (GMPLS, *Generalized MPLS*).

Un élément important de TE inter domaines est que les informations de TE ne sont pas partagées entre domaines pour des raisons d'adaptabilité et de confidentialité ([RFC4105] et [RFC4216]). Donc, un seul PCE a peu de chances d'être capable de calculer un chemin inter domaines complet.

Deux scénarios de calcul de chemin peuvent être utilisés pour les LSP TE inter domaines : un en utilisant le calcul de chemin par domaine (défini dans la [RFC5152]) et l'autre en utilisant une technique de calcul de chemin fondée sur le PCE avec coopération entre PCE (comme décrit dans la [RFC4655]). Dans ce second cas, les chemins pour les LSP inter domaines peuvent être calculés par coopération entre les PCE dont chacun calcule un segment du chemin à travers un domaine. Une telle procédure de calcul de chemin est décrite dans la [RFC5441].

Si la confidentialité est requise entre les domaines (comme ce serait très probablement le cas entre des systèmes autonomes (AS, *Autonomous System*) appartenant à des fournisseurs de service différents) alors les PCE coopérants ne peuvent pas échanger les segments de chemin ou autrement le PCE receveur et le client de calcul de chemin (PCC, *Path Computation Client*) seraient capables de voir les bonds individuels à travers un autre domaine, violant donc l'exigence de confidentialité déclarée dans les [RFC4105] et [RFC4216]. On définit la partie de chemin qu'on souhaite garder confidentielle comme le segment de chemin confidentiel (CPS, *Confidential Path Segment*).

Un mécanisme pour préserver la confidentialité du CPS est que le PCE retourne un chemin contenant un bond lâche au lieu du segment qui doit rester confidentiel. Le concept de bonds lâches et stricts pour le chemin d'un LSP TE est décrit dans la [RFC3209]. Le protocole de communication d'élément de calcul de chemin (PCEP, *Path Computation Element Communication Protocol*) défini dans la [RFC5440] prend en charge l'utilisation de chemins avec des bonds lâches, et c'est une décision de politique locale à un PCE si il retourne un chemin explicite complet avec des bonds stricts ou utilise des bonds lâches. Noter qu'une demande de calcul de chemin peut demander un chemin explicite avec des bonds stricts ou peut permettre de bonds lâches, comme détaillé dans la [RFC5440].

L'option de retourner un bond lâche au lieu du CPS peut être réalisée sans autres extensions à PCEP ou au protocole de signalisation. Si des bonds lâches sont utilisés, les LSP TE sont signalés normalement ([RFC3209]) et quand un bond lâche est rencontré dans le chemin explicite, il est résolu en effectuant un calcul de chemin secondaire pour atteindre la ou les ressources identifiées par le bond lâche. Étant donnée la nature de la coopération entre les PCE dans le calcul du chemin original, ce calcul secondaire se produit à un routeur de commutation d'étiquettes (LSR, *Label Switching Router*) ou en son nom à une frontière de domaine (c'est-à-dire, à un routeur de bordure de zone (ABR, *Area Border Router*) ou à un routeur de bordure d'AS (ASBR, *AS Border Router*)) et le chemin est développé comme décrit dans la [RFC5152].

Le modèle de calcul fondé sur le PCE est particulièrement utile pour déterminer des chemins inter domaines mutuellement disjoints comme cela pourrait être exigé pour la protection du service [RFC5298]. Une seule demande de calcul de chemin est utilisée. Cependant, si des bonds lâches sont retournés, le chemin de chaque LSP TE doit être recalculé aux frontières de domaine lorsque les LSP TE sont signalés, et comme la signalisation de LSP TE se fait indépendamment pour chaque LSP TE, les chemins disjoints ne peuvent pas être garantis parce que les LSR chargés d'étendre les objets de chemin explicite

(ERO, *Explicit Route Object*) ne sont pas synchronisés. Donc, si la technique du bond lâche est utilisée sans autre extension, la confidentialité du segment de chemin et la diversité de chemin sont des exigences mutuellement incompatibles.

Le présent document définit la notion de clé de chemin (Path-Key) qui est un jeton remplaçant un segment de chemin dans un chemin explicite. La Path-Key est codée comme sous objet de clé de chemin (PKS, *Path-Key Subobject*) retourné dans le message de réponse de calcul de chemin PCEP (PCRep, *PCEP Path Computation Reply*) ([RFC5440]). À réception du chemin calculé, le PKS va être porté dans un message Path RSVP-TE (RSVP-TE [RFC3209] et [RFC5553]) durant la signalisation.

Le BNF dans ce document suit le format décrit dans la [RFC5511].

On notera que le terme "path-key" utilisé dans ce document se réfère à un identifiant alloué par un PCE pour représenter un segment d'un chemin calculé. Ce terme n'a pas de relation avec le terme de "clé cryptographique" utilisé dans certains documents qui décrivent des mécanismes de sécurité.

### 1.1 Terminologie

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119],.

Le présent document utilise la terminologie et les acronymes suivants :

AS *(Autonomous System)* : système autonome

ASBR *(Autonomous System Border Router)* : routeur de bordure de système autonome utilisé pour connecter à un autre AS d'un même fournisseur de service ou d'un fournisseur de service différent via une ou plusieurs liaisons d'inter-connexion entre les AS.

CPS *(Confidential Path Segment)* : segment de chemin confidentiel. Un segment de chemin qui contient des nœuds et liaisons que la politique de l'AS exige de ne pas divulguer en dehors de l'AS.

LSP TE Inter-AS : LSP TE qui traverse une frontière d'AS.

LSR *(Label Switching Router)* : routeur de commutation d'étiquettes.

LSP *(Label Switched Path)* : chemin de commutation d'étiquettes.

PCC *(Path Computation Client)* : cleint de calcul de chemin. Toute application cliente qui demande qu'un calcul de chemin soit effectué par un élément de calcul de chemin.

PCE *(Path Computation Element)* : élément de calcul de chemin. Entité (composant, application ou nœud du réseau) qui est capable de calculer un chemin du réseau sur la base d'un graphe du réseau et d'appliquer des contraintes de calcul.

LSP TE *(Traffic Engineering Label Switched Path)* ; chemin de commutation d'étiquettes d'ingénierie du trafic.

## 2. Solution Path-Key

La solution Path-Key peut être appliquée dans le contexte du calcul de chemin fondé sur PCE comme suit. Un PCE calcule un segment de chemin relatif à un domaine particulier et remplace tous les CPS dans le chemin rapporté au PCC demandeur (ou un autre PCE) par un ou plusieurs sous objets appelés des PKS. Le LSR frontière d'entrée de chaque CPS DEVRAIT être spécifié en utilisant son identifiant de routeur TE comme un bond dans le chemin retourné précédant immédiatement le CPS, et d'autres sous objets PEUVENT être inclus dans le chemin immédiatement avant le bond qui identifie le LSR frontière pour indiquer les choix de liaisons et d'étiquettes. Lorsque deux PKS sont fournis à la suite sans nœuds intermédiaires, le nœud d'entrée au second CPS PEUT faire partie du premier CPS et n'a pas besoin d'être explicitement présent dans le chemin retourné. Le nœud de sortie d'un CPS PEUT être présent comme un bond strict suivant immédiatement le PKS.

### 2.1 Mode de fonctionnement

Durant le calcul de chemin, quand la politique locale impose la préservation de la confidentialité pour tout ou partie des segments de chemin à calculer ou si c'est demandé explicitement par la demande de calcul de chemin, le PCE associe une path-key au chemin calculé pour le CPS, place son propre identifiant (son PCE ID comme défini au paragraphe 3.1) avec la path-key dans un PKS, et insère l'objet PKS dans le chemin retourné au PCC ou PCE demandeur immédiatement après le sous objet qui identifie (en utilisant l'identifiant de routeur TE) le LSR qui va étendre le PKS en bonds explicites du chemin. Cela va généralement être le LSR qui est le point de départ du CPS. Le PCE qui génère un PKS DEVRAIT mémoriser le segment de chemin calculé et la path-key pour restitution ultérieure. Une politique locale DEVRAIT être utilisée pour déterminer combien de temps conserver ces informations mémorisées, et si il faut éliminer les informations après l'interrogation en utilisant les procédures décrites ci-dessous. Il est RECOMMANDÉ qu'un PCE mémorise le PKS pendant 10 minutes.

Une valeur de path-key a pour portée le PCE qui l'a calculée comme identifié par le PCE-ID porté dans le PKS. Un PCE NE DOIT PAS ré-utiliser une valeur de path-key pour représenter un nouveau CPS pendant au moins 30 minutes après l'élimination des la précédente utilisation de la même path-key. Un PCE qui n'est pas capable de conserver les informations sur les valeurs de path-key précédemment utilisées sur un redémarrage DEVRAIT utiliser un autre mécanisme pour garantir l'unicité des valeurs de path-key comme d'incorporer un horodatage ou un numéro de version dans la path-key.

Un LSR d'extrémité de tête qui est un PCC convertit le chemin retourné par un PCE en un objet de chemin explicite (ERO) qu'il inclut dans le message Path du protocole de réservation de ressources (RSVP, *Resource Reservation Protocol*). Si le chemin retourné par le PCE contient un PKS, celui-ci est inclus dans l'ERO. Comme tout autre sous objet, le PKS est passé de façon transparente de bond en bond, jusqu'à ce qu'il devienne le premier sous objet dans l'ERO. Cela va se produire au début du CPS, qui va généralement être la frontière du domaine. Le PKS DOIT être précédé par un sous objet ERO identifiant le LSR qui doit étendre le PKS. Cela signifie que (suivant les règles pour le traitement de l'ERO décrites dans la [RFC3209]) le PKS ne va pas être rencontré dans le traitement d'ERO jusqu'à ce que l'ERO soit traité par le LSR qui est capable de traiter correctement le PKS.

Un LSR qui rencontre un PKS quand il essaye d'identifier le prochain bond restitue le PCE-ID provenant du PKS et envoie un message Demande de calcul de chemin (PCReq, *Path Computation Request*) comme défini dans la [RFC5440] au PCE identifié par le PCE-ID qui contient l'objet path-key.

À réception du message PCReq, le PCE identifie le segment de chemin calculé en utilisant la path-key fournie, et retourne le segment de chemin précédemment calculé sous la forme de bonds explicites en utilisant un objet ERO contenu dans la réponse de calcul de chemin (PCRep, *Path Computation Reply*) au nœud demandeur comme défini dans la [RFC5440]. Le nœud demandeur insère les bonds explicites dans l'ERO et continue de traiter l'établissement du LSP TE conformément à la [RFC3209].

### 2.2 Exemple

La Figure 1 montre une simple topologie à deux AS avec un PCE responsable du calcul de chemin dans chaque AS. Un LSP est demandé à partir du LSR d'entrée dans un AS au LSR de sortie dans l'autre AS. L'entrée, agissant comme PCC, envoie une demande de calcul de chemin à PCE-1. PCE-1 est incapable de calculer un chemin de bout en bout et invoque PCE-2 (éventuellement en utilisant les techniques décrites dans la [RFC5441]). PCE-2 calcule un segment de chemin de ASBR-2 à la sortie comme {ASBR-2, C, D, Sortie}. Il pourrait repasser ce segment de chemin à PCE-1 en entier, ou il pourrait renvoyer le chemin {ASBR-2, Sortie} lorsque le second bond est un bond lâche.

Cependant, afin de protéger la confidentialité de la topologie dans le second AS tout en spécifiant le chemin complet, PCE-2 peut envoyer à PCE-1 un segment de chemin exprimé comme {ASBR-2, PKS, Sortie} où le PKS est un sous objet Path-Key comme défini dans le présent document. Dans ce cas, PCE-2 a identifié le segment {ASBR-2, C, D, Sortie} comme un segment de chemin confidentiel (CPS, *Confidential Path Segment*). PCE-1 va calculer le segment de chemin dont il est responsable, et va fournir le chemin complet au PCC comme {Entrée, A, B, ASBR-1, ASBR-2, PKS, Sortie}.

La signalisation se passe normalement dans le premier AS, mais quand le message Path atteint ASBR-2, le prochain bond est le PKS, et cela doit être étendu avant que la signalisation puisse progresser. ASBR-2 utilise les informations dans le PKS pour demander à PCE-2 un segment de chemin, et PCE-2 va retourner le segment {ASBR-2, C, D, Sortie} permettant à la signalisation de continuer d'établir le LSP.

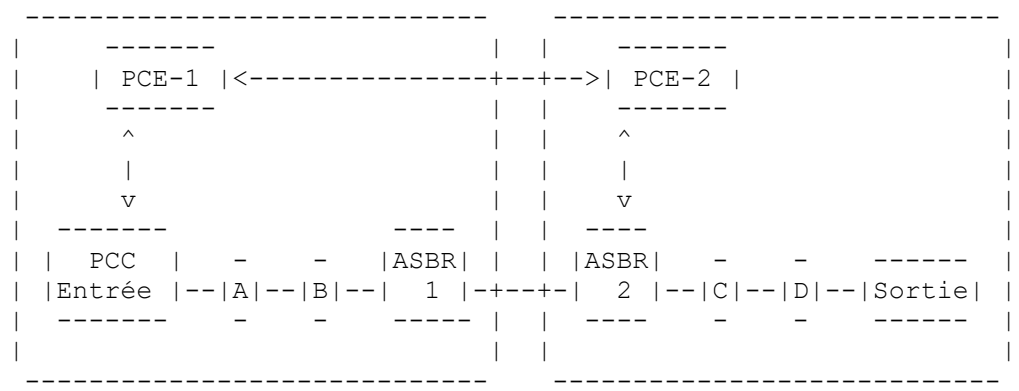



**Figure 1 : Réseau simple pour montrer l'utilisation de PKS**

## 3. Extensions au protocole PCEP

### 3.1 Path-Key dans les messages PCRep

Les Path-Key sont portées dans les messages PCReq et PCRep au titre des divers objets qui portent des définitions de chemin. En particulier, une Path-Key est portée dans l'objet Chemin explicite (ERO) sur les messages PCRep.

Dans tous les cas, le Path-Key est porté dans un sous objet Path-Key (PKS, *Path-Key Subobject*).

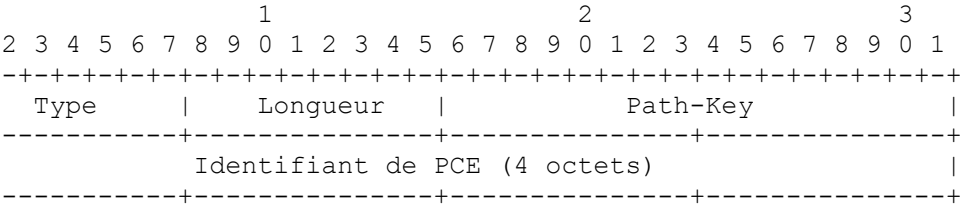
Le PKS est un sous objet de longueur fixe contenant un Path-Key et un PCE-ID. Le Path-Key est un identifiant, ou jeton utilisé pour représenter le CPS dans le contexte du PCE identifié par le PCE-ID. Le PCE-ID identifie le PCE qui peut décoder le Path-Key en utilisant un identifiant qui est unique dans le domaine que sert le PCE. Le PCE-ID doit être transposé en une adresse IPv4 ou IPv6 accessible du PCE par le premier nœud du CPS (généralement un routeur de bordure de domaine) et un PCE PEUT utiliser une de ses adresses IP accessibles comme PCE-ID. Autrement, et pour fournir plus de sécurité (voir la Section 5) ou augmenter la confidentialité, selon la politique du domaine local, le PCE PEUT utiliser un autre identifiant qui est seulement dans la portée du domaine.

Pour permettre que les adresses IPv4 et IPv6 soient portées, deux sous objets sont définis dans les paragraphes suivants.

Le sous objet Path-Key peut être présent dans l'ERO PCEP ou dans l'objet PCEP PATH-KEY (voir le paragaphe 3.2).

#### 3.1.1 PKS avec identifiant de PCE de 32 bits

Le type de sous objet pour le PKS avec l'identifiant de PCE de 32 bits est 64. Le format de ce sous objet est comme suit :




L : le bit L NE DEVRAIT PAS être établi, afin que le sous objet représente un bond strict dans le chemin explicite.

Type : le type de sous objet pour un Path-Key avec un identifiant de PCE de 32 bits (64).

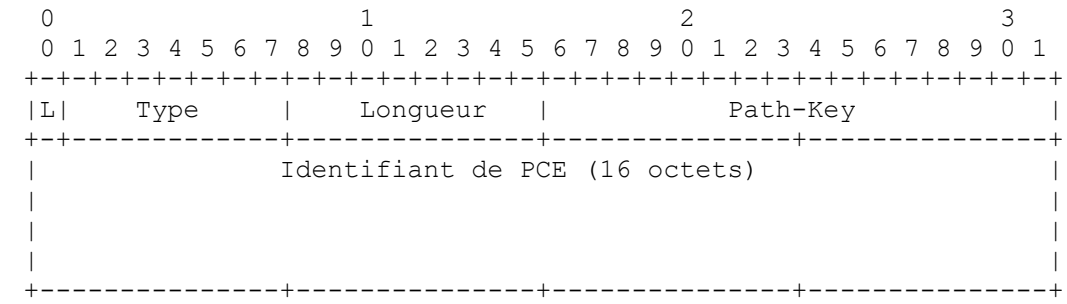
Longueur : Longueur contient la longueur totale du sous objet en octets, incluant les champs Type et Longueur. La longueur est toujours 8.

Identifiant de PCE : identifiant de 32 bits du PCE qui peut décoder cette clé de chemin. L'identifiant DOIT être unique dans la portée du domaine que traverse le CPS, et DOIT être compris par le LSR qui va agir comme PCC pour l'expansion du PKS. L'interprétation de l'identifiant de PCE est soumise à la politique du domaine local. Il PEUT être une adresse IPv4 du PCE qui est toujours accessible, et PEUT être une adresse qui est restreinte au domaine dans lequel se tient le LSR

invoqué pour étendre le CPS. D'autres valeurs qui n'ont pas de signification en-dehors du domaine (par exemple, l'identifiant de routeur du PCE) PEUVENT être utilisées pour augmenter la sécurité ou la confidentialité (voir la Section 5).

### 3.1.2 PKS avec identifiant de PCE de 128 bits

Le type de sous objet pour le PKS avec un identifiant de PCE de 128 bits est 65. Le format du sous objet est comme suit .




L : comme ci-dessus.

Type : type de sous objet pour une clé de chemin avec un identifiant de PCE de 128 bits (65).

Longueur : Longueur contient la longueur totale du sous objet en octets, incluant les champs Type et Longueur. La longueur est toujours 20.

Identifiant de PCE : identifiant de 128 bits du PCE qui peut décoder cette clé de chemin. L'identifiant DOIT être unique dans la portée du domaine que traverse le CPS, et DOIT être compris par le LSR qui va agir comme PCC pour l'expansion du PKS. L'interprétation de l'identifiant de PCE est soumise à la politique du domaine local. Il PEUT être une adresse IPv6 du PCE qui est toujours accessible, mais PEUT être une adresse qui est restreinte au domaine dans lequel se tient le LSR invoqué pour étendre le CPS. D'autres valeurs qui n'ont pas de signification en-dehors du domaine (par exemple, l'identifiant de routeur TE IPv6) PEUVENT être utilisées pour augmenter la sécurité (voir la Section 5).

## 3.2 Déverrouillage des Path-Key

Quand un nœud du réseau a besoin de décoder une clé de chemin afin de pouvoir continuer la signalisation pour un LSP, il doit envoyer une PCReq au PCE désigné. La PCReq définie dans la [RFC5440] doit être modifiée pour prendre en charge cet usage, qui diffère de la demande normale de calcul de chemin. À cette fin, un nouveau fanion est défini pour montrer que la PCReq se rapporte à l'expansion d'un PKS, et un nouvel objet est défini pour porter le PKS dans la PCReq. Il en résulte une mise à jour du BNF pour le message. Le BNF utilisé dans ce document est celui décrit dans la [RFC5511].

### 3.2.1 Bit Path-Key

La [RFC5440] définit l'objet Paramètres de demande (RP, *Request Parameters*) qui est utilisé pour spécifier diverses caractéristiques de la demande de calcul de chemin (PCReq, *Path Computation Request*).

Dans ce document, on définit un nouveau bit appelé le bit Path-Key comme suit. Voir au paragraphe 7.3 l'allocation par l'IANA du numéro de bit approprié.

Bit Path-Key : quand il est établi, le PCC demandeur exige la restitution d'un segment de chemin confidentiel (CPS) qui correspond au PKS porté dans un objet PATH-KEY dans la demande de calcul de chemin. Le bit Path-Key DOIT être à zéro quand la demande de calcul de chemin est sans relation avec une restitution de CPS.

### 3.2.2 Objet PATH-KEY

Quand un PCC a besoin d'étendre une clé de chemin afin d'étendre un CPS, il produit une PCReq au PCE identifié dans le PKS dans l'ERO RSVP-TE qu'il traite. Le PCC fournit le PKS à étendre dans un objet PATH-KEY dans le message PCReq.

L'objet PATH-KEY est défini comme suit :
La classe d'objet PATH-KEY est 16.
Le type d'objet Path-Key est 1.
L'objet PATH-KEY DOIT contenir au moins un sous objet Path-Key (voir le paragraphe 3.1). Le premier PKS DOIT être traité par le PCE. Les sous objets suivants DEVRAIENT être ignorés.

### 3.2.3 Message Demande de calcul de chemin (PCReq) avec Path-Key

Le format d'un message PCReq incluant un objet PATH-KEY est inchangé comme suit :

<Message PCReq>::= <En-tête commun> [<SVEC-list>] <request-list>

où :
<svec-list>::=<SVEC>[<svec-list>]
<request-list>::=<request>[<request-list>]

Pour prendre en charge l'utilisation du message pour étendre un PKS, la définition de <request> est modifiée comme suit :

<request>::= <RP> <segment-computation> | <path-key-expansion>

où :
<segment-computation> ::= <END-POINTS>
[<LSPA>]
[<BANDWIDTH>]
[<BANDWIDTH>]
[<metric-list>]
[<RRO>]
[<IRO>]
[<LOAD-BALANCING>]
<path-key-expansion> ::= <PATH-KEY>

Donc, le format du message à utiliser dans le calcul de chemin normal n'est pas modifié.

## 4. Mode de fonctionnement PCEP pou l'expansion de Path-Key

La restitution du chemin explicite (le CPS) associé à un PKS par un PCC n'est pas différente de celle de toute autre demande de calcul de chemin avec l'exception que le message PCReq DOIT contenir un objet PATH-KEY et que le bit Path-Key de l'objet RP DOIT être établi. À réception d'une PCRep contenant un CPS, le PCC demandeur DEVRAIT insérer le CPS dans l'ERO qu'il va signaler, en accord avec la politique locale.

Si le PCE receveur ne se reconnaît pas lui-même comme identifié par l'identifiant de PCE porté dans le PKS, il PEUT transmettre le message PCReq à un autre PCE en accord avec la politique locale. Si le PCE ne transmet pas de telles PCReq, il DOIT répondre avec un message PCRep contenant un objet NO-PATH.

Si le PCE receveur se reconnaît lui-même, mais ne peut pas trouver le CPS concerné, ou si la restitution du CPS n'est pas permise par sa politique, le PCE DOIT envoyer un message PCRep qui contient un objet NO-PATH. Le TLV NO-PATH-VECTOR DEVRAIT être utilisé comme décrit dans la [RFC5440] et un nouveau numéro de bit (voir le paragraphe 7.4) est alloué pour indiquer "Ne peut pas étendre le PKS".

À réception d'une réponse négative, le LSR demandeur DOIT faire échouer l'établissement de LSP et DEVRAIT utiliser les procédures associées à la défaillance d'expansion de bond lâche [RFC3209].

## 5. Considérations sur la sécurité

Le présent document décrit le tunnelage des informations de chemin confidentiel à travers un domaine qui n'est pas de confiance (comme un AS). De nombreuses considérations de sécurité s'appliquent à PCEP et RSVP-TE.

Les problèmes incluent :

- La confidentialité du CPS (d'autres éléments de réseau peuvent-ils sonder l'expansion des clés de chemin, éventuellement au hasard ?).

- L'authenticité de la path-key (résilience à l'altération par des intermédiaires, résilience à une fausse expansion des path-key).

- Résilience aux attaques de déni de service (insertion de path-key parasites ; inondation de demandes d'expansion de path-key boguées).

La plupart des interactions exigées par cette extension sont en point à point, peuvent être authentifiées et rendues sûres comme décrit dans les [RFC5440] et [RFC3209]. Ces interactions incluent :
- demande de PCC à PCE
- la ou les demandes de PCE à PCE
- la ou les réponses de PCE à PCE
- réponse de PCE à PCC
- demande et réponse de LSR à LSR. Noter qu'un LSR félon pourrait modifier l'ERO et insérer ou modifier les Path-Key. Il en résulterait qu'un LSR (en aval dans l'ERO) envoie des demandes de décodage à un PCE. Ceci est actuellement un problème plus vaste avec RSVP. Le LSR félon est un problème qui existe avec RSVP et ne sera pas traité ici.
- demande de LSR à PCE. Noter que le PCE peut vérifier que le LSR qui demande le décodage est le LSR de tête du Path-Key. Cela contient largement le précédent problème de déni de service plutôt qu'un problème de sécurité. Un LSR félon peut produire des demandes de décodage aléatoires, mais cela revient seulement à du déni de service.
- réponse de PCE à LSR.

Donc, les problèmes majeurs de sécurité peuvent être réglés en utilisant les techniques standard pour sécuriser et authentifier les communications en point à point. De plus, il est recommandé que le PCE qui fournit une réponse de décodage devrait vérifier que le LSR qui a produit la demande de décodage est l'extrémité de tête du segment d'ERO décodé.

Plus de protection peut être fournie en utilisant un identifiant de PCE pour identifier le PCE décodeur qui soit significatif seulement dans le domaine qui contient le LSR à la tête du CPS. Ce peut être une adresse IP qui est seulement accessible de l'intérieur du domaine, ou une valeur non d'adresse. La première exige une configuration de politique sur les PCE ; la seconde exige une politique à l'échelle du domaine.

## 6. Considérations de gestion

### 6.1 Contrôle de fonction par configuration et politique

Le traitement d'un segment de chemin comme un CPS, et sa substitution dans un ERO PCRep par un PKS, est une fonction qui DOIT être sous le contrôle d'un opérateur et d'une politique où un PCE prend en charge la fonction. L'opérateur DOIT avoir la capacité de spécifier quels segments de chemin sont à remplacer et dans quelles circonstances. Par exemple, un opérateur pourrait établir une politique qui déclare que tout segment de chemin pour le domaine de l'opérateur va être remplacé par un PKS quand la PCReq a été produite de l'extérieur du domaine.

L'opération d'extension de PKS exige que les path-key soient conservées par le PCE qui les produit pour être disponibles à la restitution par un LSR (agissant comme un PCC) ultérieurement. Mais il est possible qu'une demande de restitution ne soit jamais faite, donc une bonne gestion exige qu'un temporisateur règle l'élimination des path-key non voulues. Une valeur par défaut pour ce temporisateur est suggérée au paragrahe 2.1. Les mises en œuvre DEVRAIENT donner la possibilité que cette valeur soit outrepassée par configuration ou par la politique de l'opérateur.

Après qu'un PKS a été étendu en réponse à une demande de restitution, il peut être précieux de conserver la path-key et le CPS à des fins de débogage. Une telle rétention NE DEVRAIT PAS être le comportement par défaut d'une mise en œuvre, mais PEUT être disponible en réponse à une demande de l'opérateur.

Une fois qu'une path-key a été éliminée, la valeur de path-key NE DEVRAIT PAS être immédiatement disponible pour réutilisation pour un nouveau CPS car cela pourrait conduire à une mauvaise utilisation accidentelle. Une valeur de temporisation par défaut est suggérée au paragraphe 2.1. Les mises en œuvre DEVRAIENT fournir la capacité que cette valeur soit outrepassée par configuration ou par la politique de l'opérateur.

Un PCE doit établir une valeur de PCE-ID dans chaque PKS qu'il crée afin que les PCC puissent correctement l'identifier et envoyer des messages PCReq pour étendre le PKS à un segment de chemin. Une mise en œuvre de PCE DEVRAIT permettre le contrôle par l'opérateur ou par la politique de la valeur à utiliser comme identifiant de PCE. Si le PCE permet d'utiliser des valeurs d'identifiant de PCE qui ne sont pas des adresses acheminables, les PCC DOIVENT être configurables (par l'opérateur ou par la politique) pour permettre aux PCC de transposer l'identifiant de PCE en une adresse acheminable du PCE. Une telle transposition peut être algorithmique, procédurale (par exemple, transposer un identifiant de PCE égal à l'identifiant de routeur IGP en une adresse acheminable) ou configurée au moyen d'un tableau de transposition local ou distant.

### 6.2 Modèles d'information et de données

Un module de MIB pour PCEP est déjà défini dans la [RFC7420]. Les éléments configurables mentionnés au paragraphe 6.1 DOIVENT être ajoutés comme objets lisibles dans le module et DEVRAIENT être ajoutés comme objets d'écriture.

Un nouveau module de MIB DOIT être créé pour permettre l'inspection des clés de chemin. Pour un PCE donné, ce module de MIB DOIT fournir une transposition de clé de chemin à segment de chemin (c'est-à-dire, une liste de bonds) et DOIT fournir d'autres informations incluant :

- L'identité du PCC qui a produit la demande originale qui a conduit à la création de la path-key.
- L'identifiant de demande de la PCReq originale.
- Si la path-key a déjà été restituée, et si elle l'a été, par quel PCC.
- Dans combien de temps le segment de chemin associé à la path-key va être éliminé.
- Pendant combien de temps la path-key va être disponible pour réutilisation.

### 6.3 Détection et surveillance de vie

Les procédures du présent document étendent PCEP, mais n'introduisent pas de nouvelles interactions entre entités du réseau. Donc, aucune nouvelle détection ou surveillance de vie n'est nécessaire.

Il est possible qu'un LSR d'extrémité de tête à qui a été donné un chemin incluant des PKS remplaçant des CPS spécifiques veuille savoir si les clés de chemin sont encore valides (ou périmées). Cependant, plutôt que d'introduire un mécanisme pour interroger le PCE responsable du PKS, il est considéré plus pragmatique de simplement signaler le LSP associé.

### 6.4 Vérification de fonctionnement correct

Les procédures de ce document étendent PCEP, mais n'introduisent pas de nouvelles interactions entre les entités de réseau. Donc, aucun nouvel outil pour vérifier le fonctionnement correct n'est exigé.

Un PCE DEVRAIT tenir des compteurs et des journaux des événements suivants qui pourraient indiquer un fonctionnement incorrect (ou pourraient indiquer des problèmes de sécurité).

- Tentatives d'étendre une path-key inconnue.
- Tentatives d'étendre une path-key expirée.
- Tentatives dupliquées d'étendre la même path-key.
- Expiration de path-key sans tentative de l'étendre.

### 6.5 Exigences sur d'autres protocoles et composants fonctionnels

Les procédures décrites dans ce document exigent que les LSR signalent les PKS comme défini dans la [RFC5553]. Noter que les seuls changements aux LSR sont aux PCC. Précisément, des changements sont seulement nécessaires aux LSR d'extrémité de tête qui construisent des messages Path RSVP-TE contenant des sous objets Path-Key dans leurs ERO, et les LSR qui découvrent de tels sous objets comme prochains bonds et doivent les étendre. Les autres LSR dans le réseau, même si ils sont sur le chemin du LSP, ne vont pas être appelés à traiter le PKS.

### 6.6 Impact sur le fonctionnement du réseau

Tout comme les aspects de sécurité et de confidentialé visés par l'utilisation du PKS, il peut y avoir des avantages d'adaptabilité associés aux procédures décrites dans ce document. Par exemple, un seul PKS dans un chemin explicite peut se substituer à de nombreux sous objets et peut réduire la taille globale du message de façon correspondante. Dans certaines circonstances, comme quand le chemin explicite contient plusieurs sous objets pour chaque bond (incluant des identifiants

de nœud, des identifiants de liaison TE, des identifiants de liaison composante pour chaque direction d'un LSP bidirectionnel, et des identifiants d'étiquettes pour chaque direction d'un LSP bidirectionnel) ou quand le LSP est un LSP de point à multipoints, cette amélioration de l'adaptabilité peut être très significative.

Noter qu'un PCE ne va pas fournir de PKS sauf si il sait que le LSR qui va recevoir le PKS par la signalisation va être capable de le traiter. De plus, comme noté au paragraphe 6.5, seuls les LSR spécifiquement appelés à étendre le PKS vont être obligés de traiter les sous objets durant la signalisation. Donc, les seuls problèmes de rétro compatibilité associés aux procédures introduites dans ce document surviennent quand un LSR d'extrémité de tête reçoit une PCRep avec un ERO contenant un PKS, et qu'il ne sait pas comment coder cela dans la signalisation.

Comme le PCE qui a inséré le PKS est obligé de garder le CPS confidentiel, le LSR d'extrémité de tête traditionnel ne peut pas être protégé. Il doit soit faire échouer l'établissement de LSP, soit demander un nouveau calcul de chemin évitant le domaine qui l'a fourni avec des sous objets inconnus.

## 7. Considérations relatives à l'IANA

L'IANA alloue des valeurs aux paramètres PCEP dans les registres définis dans la [RFC5440]. L'IANA a fait les allocations supplémentaires suivantes.

### 7.1. Nouveaux sous objets pour l'objet ERO

L'IANA avait précédemment alloué une classe d'objet et un type d'objet à l'ERO porté dans les messages PCEP [RFC5440]. L'IANA tient aussi une liste des types de sous objet valides pour être inclus dans l'ERO.

L'IANA a alloué deux nouveaux types de sous objet à inclure dans l'ERO comme suit :

| Numéro | Type de sous objet | Référence |
|---|---|---|
| 64 | Path-Key avec ID PCE de 32 bits | [RFC5520] |
| 65 | Path-Key avec ID PCE de 128 bits | [RFC5520] |

### 7.2 Nouvel objet PCEP

L'IANA a alloué une nouvelle classe d'objet dans le registre des objets PCEP comme suit :

| Classe d'objet | Nom | Type d'objet | Nom | Référence |
|---|---|---|---|---|
| 16 | PATH-KEY | 1 | Path-Key | [RFC5520] |

Sous objets
Cet objet peut porter les sous objets suivants comme défini pour l'objet ERO.

| | | |
|---|---|---|
| 64 | Path-Key avec PCE ID de 32 bits | [RFC5520] |
| 65 | Path-Key avec PCE ID de 128 bits | [RFC5520] |

### 7.3 Nouveau fanion de bit Objet RP

L'IANA tient un registre des fanions de bits portés dans l'objet RP PCEP comme défini dans la [RFC5440]. L'IANA a alloué un nouveau fanion de bit comme suit :

| Numéro de bit | Hexadécimal | Nom | Référence |
|---|---|---|---|
| 23 | 0x000017 | Path-Key (P-bit) | [RFC5520] |

### 7.4 Nouveau fanion de bit TLV NO-PATH-VECTOR

L'IANA tient un registre des fanions de bits portés dans le TLV PCEP NO-PATH-VECTOR dans l'objet PCEP NO-PATH comme défini dans la [RFC5440]. L'IANA a alloué un nouveau fanion de bit comme suit :

| Numéro de bit | Fanion de nom | Référence |
|---|---|---|
| 27 | Échec d'expansion PKS | [RFC5520] |

# 8. Références

## 8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC5440] JP. Vasseur et autres, "Protocole de communication d'élément de calcul de chemin (PCEP)", mars 2009. *(P. S. ; MàJ par* RFC7896, RFC8253, RFC8356, RFC9488)

## 8.2 Références pour information

[RFC3209] D. Awduche, et autres, "RSVP-TE : Extensions à RSVP pour les tunnels LSP", décembre 2001. (*Mise à jour par* RFC3936, RFC4420, RFC4874, RFC5151, RFC5420, RFC6790)

[RFC4105] J.-L. Le Roux, J.-P. Vasseur et J. Boyle, "Exigences pour l'ingénierie de trafic MPLS interzones", juin 2005.

[RFC4216] R. Zhang et J.-P. Vasseur, "Exigences pour l'ingénierie de trafic MPLS entre systèmes autonomes (AS)", novembre 2005. *(Information)*

[RFC4655] A. Farrel, J.-P. Vasseur et J. Ash, "Architecture fondée sur l'élément de calcul de chemin (PCE)", août 2006.

[RFC5152] JP. Vasseur et autres, "Méthode de calcul de chemin par domaine pour établir des chemins de commutation d'étiquettes (LSP) à ingénierie du trafic inter domaine", février 2008. *(P.S.)*

[RFC5298] T. Takeda et autres, "Analyse de la récupération de chemin commuté par étiquettes (LSP) inter domaine", août 2008. *(Inf)*

[RFC5441] JP. Vasseur, éd., R. Zhang, N. Bitar, JL. Le Roux "Procédure de calcul rétro récurrent fondée sur PCE (BRPC) pour calculer le plus court chemin obligé de commutation d'étiquette à ingénierie du trafic inter-domaine", avril 2009. *(P. S.)*

[RFC5511] A. Farrel, "Forme Backus-Naur d'acheminement (RBNF) : syntaxe utilisée pour former les règles de codage dans diverses spécifications de protocole d'acheminement", avril 2009. *(P.S.)*

[RFC5553] A. Farrel, éd., R. Bradford, JP. Vasseur,"Extensions au protocole de réservation de ressource (RSVP) pour la prise en charge de la clé de chemin", mai 2009. *(P. S.)*

[RFC7420] A. Koushik, et autres, "Module de MIB du protocole de communication d'élément de calcul de chemin (PCECP)", décembre 2014. *(P.S.)*

# Remerciements

Les auteurs tiennent à remercier Eiji Oki, Ben Campbell, et Ross Callon de leurs commentaires sur ce document.

# Adresse des auteurs

Rich Bradford (éditeur)
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
mél : rbradfor@cisco.com

JP. Vasseur
Cisco Systems, Inc.
1414 Massachusetts Avenue
Boxborough, MA 01719
USA
mél : jpv@cisco.com

Adrian Farrel
Old Dog Consulting
mél : adrian@olddog.co.uk